UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

DEBRA L. BROWN, individually and on behalf of all others similarly situated, Plaintiff, v. PERRY JOHNSON & ASSOCIATES, INC. AND NORTHWELL HEALTH, INC. Defendants.	CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Debra L. Brown ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class," as more fully defined below), brings this class action against Defendants Perry Johnson & Associates, Inc. and Northwell Health, Inc. (collectively "Defendants"). Plaintiff makes the following allegations upon personal knowledge as to her own acts, upon information and belief and her attorneys' investigation as to all other matters, and allege as follows:

INTRODUCTION

1. This action arises out of a targeted cyberattack and data breach caused by Defendants' failure to secure and safeguard Plaintiff's and millions of other individuals' personally identifying information ("PII") and personal health

information ("PHI"), including names, Social Security numbers ("SSNs"), dates of birth, addresses, medical record numbers, encounter numbers, medical information, and dates/times of service.

2. Defendant Northwell Health, Inc. ("Northwell") is the largest health system in New York and, as part of the healthcare services it renders, it collects and stores the PII and PHI of its patients.

3. Perry Johnson & Associates, Inc. ("PJ&A") is a third-party vendor of health information technology solutions used by Northwell. To facilitate the services rendered by PJ&A, Northwell shared the sensitive PII and PHI of their patients with PJ&A.

4. Between approximately March 27, 2023 and May 2, 2023, an unauthorized third-party gained access to PJ&A's network system and obtained files containing the PII and PHI of Northwell's current and former patients (the "Data Breach").

5. Defendants owed a duty to Plaintiff and the other Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Northwell's patients' PII and PHI from unauthorized access and disclosure.

6. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and the other Class members' PII and PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII and PHI was exposed as a result of the Data Breach, which occurred between approximately March 27, 2023, and May 2, 2023.

7. Plaintiff, on behalf of herself and the Class, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of New York state statutes, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

A. Plaintiff

8. Plaintiff Debra L. Brown is a citizen of the state of New York.

9. Plaintiff Brown obtained healthcare or related services from Northwell. As a condition of receiving services, Northwell required Plaintiff Brown to provide it with her PII and PHI.

10. Plaintiff Brown received a notice from Defendant PJ&A dated November 3, 2023 notifying her that her PII and PHI were compromised in the Data Breach.[1]

11. Based on representations made by Northwell, Plaintiff Brown believed Northwell had implemented and maintained reasonable security procedures and practices to protect her PII and PHI. With this belief in mind, Plaintiff Brown provided her PII and PHI to Northwell in connection with receiving healthcare services provided by Northwell.

12. At all relevant times, Defendants Northwell and PJ&A stored and maintained Plaintiff Brown's PII and PHI on their network systems.

13. Plaintiff Brown takes great care to protect her PII and PHI. Had Plaintiff Brown known that Northwell does not adequately protect the PII and PHI in its possession, including by contracting with companies that do not adequately protect the PII and PHI in their possession, she would not have obtained healthcare services from Northwell or agreed to entrust it with her PII and PHI.

14. As a direct result of the Data Breach, Plaintiff Brown has suffered injury and damages including, without limitation, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII and PHI; loss of the potential value of her

[1] See Plaintiff Brown's Notice of Data Breach, attached herein as Exhibit A.

PII and PHI; and overpayment for services that did not include adequate data security. Additionally, Plaintiff Brown has had to spend valuable time responding to the Data Breach that she would have otherwise spent on other activities, including but not limited to work and/or recreation.

B. Defendants

15. Defendant Northwell Health, Inc. is a New York not-for-profit corporation with its principal place of business at 2000 Marcus Ave., New Hyde Park, NY 11042.

16. Defendant Perry Johnson & Associates, Inc. is a Nevada corporation with its headquarters in Troy, Michigan.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because there are 100 or more Class members, Plaintiff and at least one Class member is a citizen of a state that is diverse from at least one Defendants' citizenships, and the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

18. This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc. because it is a corporation headquartered in Michigan. Michigan is the physical location of many of the relevant witnesses and documents at issue, and the PJ&A servers breached in the Data Breach are located in Michigan.

19. This Court has personal jurisdiction over Defendant Northwell Health, Inc., because it transacts business within this state and makes or performs contracts within this state.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because PJ&A has its headquarters the Eastern District of Michigan, and a substantial part of the events giving rise to Plaintiff's claims arose in this District.

FACTUAL ALLEGATIONS

A. Overview of Defendants

21. Northwell is the largest health system in New York.[2] It employs more than 85,000 people at over 900 locations, including 21 hospitals.[3]

22. In the regular course of its business, Northwell collects and maintains the PII and PHI of its current and former patients. Northwell required Plaintiff and the other Class members to provide their PII and PHI as a condition of receiving healthcare services from Northwell.

23. On its website, Northwell claims "patients are our number one priority and we believe that patient privacy is an integral part of the health care we provide

[2] *About Northwell*, NORTHWELL HEALTH, https://www.northwell.edu/about-northwell (last accessed Nov. 10, 2023).

[3] *Id.*

to you."[4] Northwell states, "[t]o ensure the development of a lasting bond of trust with our patients, we have many safeguards to protect the privacy and security of your personal information."[5] Northwell further promises that "[w]e also have many policies in place to protect the privacy and security of your personal information and our employees are educated from the moment they are hired and continually after, to respect and protect our patient's privacy."[6]

24. Northwell's website contains a Notice of Privacy Practices that "explains how we fulfill our commitment to respect the privacy and confidentiality of your protected health information."[7] In the Notice, Northwell admits it is "required by law to make sure that information that identifies you is kept private."

25. The Privacy Policy includes a list of the ways Northwell may use and disclose its patients' health information, including for treatment, payment, and health care operations, among others.[8] The Privacy Policy promises that disclosures

[4] *Patient Privacy Overview*, NORTHWELL HEALTH, https://www.northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy (last accessed Nov. 10, 2023).

[5] *Id.*

[6] *Id.*

[7] *Notice of Privacy Practices*, NORTHWELL HEALTH, https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf (last accessed Nov. 10, 2023).

[8] *Id.*

not described in the Notice or permitted by law will be made only with patients' written authorization.[9]

26. PJ&A "provides medical transcription services to various healthcare organizations."[10] Northwell used PJ&A for medical transcription and dictation services.[11]

27. Plaintiff and the other Class members are current or former patients of Northwell and entrusted Northwell with their PII and PHI.

B. The Data Breach

28. Between approximately March 27, 2023 and May 2, 2023, "[a]n unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems." [12]

29. According to the Notice of Data Security Incident posted on PJ&A's website, the PII and PHI exposed in the Data Breach included names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses,

---

[9] *Id.*

[10] *Cyber Incident Notice*, PERRY JOHNSON & ASSOCS., https://www.pjats.com/downloads/Notice.pdf (last accessed Nov. 10, 2023) [hereinafter "*PJA Notice*"].

[11] *See* Kevin Vesey, *Cyberattack Targets Northwell Health Vendor; Patient Data Compromised*, NEWS12 (Nov. 9, 2023 6:52 PM), https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach; *see also* Jill McKeon, *Medical Transcription Service Data Breach Impacts Multiple Health Systems*, TECHTARGET (Nov. 16, 2023), https://healthitsecurity.com/news/medical-transcription-service-data-breach-impacts-multiple-health-systems.

[12] *PJA Notice*, *supra* note 9; *see also* Plaintiff Brown's Notice of Data Breach, Ex. A.

dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names.[13]

30. Northwell's Notice of Privacy Practices states, "[y]ou have a right to be notified in the event of a breach of the privacy of your unsecured protected health information by Northwell Health or its business associates."[14] It also promises patients that they "will be notified as soon as reasonably possible, but no later than 60 days following our discovery of the breach."[15]

31. PJ&A informed Northwell of the Data Breach on July 21, 2023,[16] but Northwell failed to notify its patients until early November 2023, over three months later.

32. Northwell's failure to promptly notify Plaintiff and the other Class members that their PII and PHI was accessed and stolen allowed the unauthorized third parties who exploited those security lapses to monetize, misuse, or disseminate that PII and PHI before Plaintiff and the other Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and the other Class

[13] *Id.*

[14] *Notice of Privacy Practices*, *supra* note 6.

[15] *Id.*

[16] Vesey, *supra* note 10.

members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

C. Defendants Knew that Criminals Target PII and PHI

33. At all relevant times, Defendants knew, or should have known, that the information they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and the other Class members' PII and PHI from cyber-attacks that Defendants should have anticipated and guarded against.

34. It is well known among companies that store sensitive personally identifying information that such information—such as the PII and PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[17]

35. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient

[17] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

records exposed.[18] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[19]

36. PII and PHI is a valuable property right.[20] The value of PII and PHI as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[23] It is so valuable to identity thieves that once PII and PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[18] *See 2023 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last accessed Nov. 10, 2023).

[19] *See id*.

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[22] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[23] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

37. As a result of the real and significant value of this data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII and PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

38. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[24] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[25]

39. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[26] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals

[24] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[25] *Id.*

[26] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[27]

40. Criminals can use stolen PII and PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[28] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[29]

41. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[30]

---

[27] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[28] Steager, *supra* note 23.

[29] *Id.*

[30] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

42. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII and PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Defendants are Covered Entities Subject to HIPAA

43. Defendants had duties to ensure that all information they collected and stored was secure, and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class members' PII and PHI.

44. Defendants are HIPAA covered entities that provide services to patients and/or healthcare and medical service providers. As a regular and necessary part of their businesses, Defendants collect the highly sensitive PII and PHI of their and their clients' patients.

45. Indeed, PJ&A recognizes the importance of its obligations under HIPAA on its own webpage, where PJ&A claims that its platform enables HIPAA compliance "through advanced technology for dictation, transcription and patient data accessibility."[31]

[31] HIPAA Compliancy, PJ&A, https://www.pjats.com/hipaa-compliancy/ (last accessed Nov. 20, 2023).

46. As covered entities under HIPAA, Defendants are required under federal and state law to maintain the strictest confidentiality of the patient's PII and PHI that they acquire, receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that PII and PHI from being accessed by unauthorized third parties.

E. Defendants' Conduct Violates HIPAA Obligations to Safeguard PII and PHI

47. Because Defendants are covered by HIPAA (see 45 C.F.R. § 160.102), they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

48. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[32] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

49. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where

[32] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

50. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

51. HIPAA requires that Defendants implement appropriate safeguards for this information.

52. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

53. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

54. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires HIPAA covered entities and their business associates, like Defendants, to provide notification following a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e. non-encrypted data—to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[33]

55. HIPAA requires covered entities to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

56. HIPAA requires covered entities to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

57. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance

[33] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/forprofessionals/breach-notification/index.html (emphasis added).

documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." See US Department of Health & Human Services, Guidance on Risk Analysis.[34]

58. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four-factor risk assessment focuses on:

(1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

[34] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and,

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[35]

59. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own Privacy Practices. Indeed, Defendants failed to:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiff's and Class members' PII and PHI;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

[35] 78 Fed. Reg. 5641-46; see also 45 C.F.R. § 164.304.

h) Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i) Conduct the Four Factor Risk Analysis following the Breach;

j) Properly send notice to Plaintiff and Class members pursuant to 45 C.F.R. §§ 164.400- 414;

k) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

l) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

60. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

61. A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

62. Defendants failed to comply with their duties under HIPAA and their own privacy policies despite being aware of the risks associated with unauthorized access of Plaintiff's and Class members' PII and PHI.

63. Defendants' Data Breach resulted from a combination of insufficiencies that indicate that Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards.

F. Defendants Fail to Comply with FTC Guidelines

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[36] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of

[36] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

data being transmitted from the system; and, have a response plan ready in the event of a breach.[37]

66. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were

[37] *Id.*

unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

69. Defendants failed to properly implement basic data security practices.

70. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. Defendants were at all times fully aware of their obligation to protect the PII and PHI of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

G. Defendants Fail to Comply with Industry Standards

72. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

73. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limitations on which employees can access sensitive data.

74. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

75. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and, ultimately, causing the Data Breach.

H. Theft of PII and PHI Has Grave and Lasting Consequences for Victims

77. Theft of PII and PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII and PHI to receive medical

treatment, start new utility accounts, and incur charges and credit in a person's name.[38] [39]

78. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[40]

79. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[41]

---

[38] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 10, 2023).

[39] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[40] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[41] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Nov. 10, 2023).

80. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[42] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[43] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII and PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[44] The FTC also warns, "[i]f the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[45]

81. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[42] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[43] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 26.

[44] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 10, 2023).

[45] *Id*.

82. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[46]

83. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a) Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b) Significant bills for medical goods and services neither sought nor received.

c) Issues with insurance, co-pays, and insurance caps.

d) Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e) Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the

[46] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f) As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g) Phantom medical debt collection based on medical billing or other identity information.

h) Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [47]

84. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[48]

I. Damages Sustained by Plaintiff and Class Members

85. Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from

[47] *See* Dixon & Emerson, *supra* note 34.

[48] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data Breach; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

86. Plaintiff brings this action as a class action pursuant to Rules 23(a), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of a class defined as:

> **Nationwide Class:** All United States residents whose PII and/or PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

and State Subclass defined as:

> **New York Subclass**: All New York residents whose PII and/or PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

87. Excluded from the Class are Defendants and any of their members, affiliates, parents, subsidiaries, officers, directors, employees, successors, or assigns; and the Court staff assigned to this case and their immediate family members.

Plaintiff reserves the right to modify or amend the Class definition, as appropriate, during the course of this litigation.

88. This action has been brought and may properly be maintained on behalf of the Class proposed herein under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

89. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The proposed Class is sufficiently numerous that individual joinder of all Class members is impracticable. Indeed, the Class size is believed to be in the millions of individuals. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

90. Commonality and Predominance—Federal Rules of Civil Procedure 23(a)(2), 23(b)(3), and 23(c)(4). This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, within the meaning of Fed. R. Civ. P. 23(a)(2) and (b)(3). Class treatment of common issues under Fed. R. Civ. P. 23(c)(4) will also materially advance the litigation. Common questions of fact and law affecting Class members include, without limitation:

a) Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and the other Class members' PII and PHI from unauthorized access and disclosure;

b) Whether Defendants had duties not to disclose the PII and PHI of Plaintiff and the other Class members to unauthorized third parties;

c) Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and the other Class members' PII and PHI;

d) Whether an implied contract existed between Plaintiff and the other Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Plaintiff's and the other Class members' PII and PHI from unauthorized access and disclosure;

e) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and the other Class members;

f) Whether Defendants breached their duties to protect Plaintiff's and the other Class members' PII and PHI; and

g) Whether Plaintiff and the other Class members are entitled to damages and the measure of such damages and relief.

91. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the other Class members' claims because Plaintiff and each of the other Class members had their PII and PHI compromised in the Data Breach. Plaintiff and the other Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

92. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other Class members who she seeks to represent, Plaintiff has retained counsel competent and experienced in complex class action litigation, including successfully litigating data breach class action cases similar to this one, and Plaintiff intends to prosecute this action vigorously. Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

93. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class against all Defendants)

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

95. Defendants owed a duty to Plaintiff and the other Class members to exercise reasonable care in safeguarding and protecting the PII and PHI in their possession, custody, or control.

96. Defendants knew or should have known the risks of collecting and storing Plaintiff's and the other Class members' PII and PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare providers that collect and store PII and PHI in recent years.

97. Given the nature of Defendants' businesses, the sensitivity and value of the PII and PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

98. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII and PHI and by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to it—including Plaintiff's and Class members' PII and PHI.

99. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII and PHI and by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and the other Class members' PII and PHI to unauthorized individuals.

100. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and the other Class members, their PII and PHI would not have been compromised.

101. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Defendants'

possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data Breach; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Nationwide Class against all Defendants)

102. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

103. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

104. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Northwell, of failing to employ reasonable measures to protect and secure PII and PHI.

105. Defendants violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, and IPIPA by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiff's and the other Class members' PII and PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtain and store, and the foreseeable consequences of a data breach involving PII and PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

106. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

107. Plaintiff and the other Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

108. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type

of harm that has been suffered by Plaintiff and the other Class members as a result of the Data Brach.

109. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI and by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and the other Class members' PII and PHI to unauthorized individuals.

110. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of harm the HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of

the PII and PHI compromised as a result of the Data Breach; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Nationwide Class against Northwell only)

111. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

112. This claim is brought by Plaintiff on behalf of all Class members who provided their PII and PHI to Northwell.

113. Plaintiff and the other Class members gave Northwell their PII and PHI in confidence, believing that Northwell would protect that information. Plaintiff and the other Class members would not have provided Northwell with this information had they known it would not be adequately protected. Northwell's acceptance and storage of Plaintiff's and the other Class members' PII and PHI created a fiduciary relationship between Northwell on the one hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, Northwell must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and the other Class members' PII and PHI.

114. Due to the nature of the relationship between Northwell on the one hand, and Plaintiff and the other Class members, on the other hand, Plaintifs and the other Class members were entirely reliant upon Northwell to ensure that their PII and PHI was adequately protected. Plaintiff and the other Class members had no way of verifying or influencing the nature and extent of Northwell's or their vendors' data security policies and practices, and Northwell were in an exclusive position to guard against the Data Breach.

115. Northwell have a fiduciary duty to act for the benefit of Plaintiff and the other Class members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to properly protect the integrity of the systems containing Plaintiff's and the other Class members' PII and PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and the other Class members' PII and PHI that they collected.

116. As a direct and proximate result of Northwell's breaches of its fiduciary duties, Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs

associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Northwell's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data Breach; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class against Northwell Only)

117. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

118. This claim is brought by Plaintiff on behalf of all Class members who provided their PII and PHI to Northwell.

119. In connection with receiving healthcare services, Plaintiff and the other Class members entered into implied contracts with Northwell.

120. Pursuant to these implied contracts, Plaintiff and the other Class members paid money to Northwell, directly or through their insurance, and provided Northwell with their PII and PHI. In exchange, Northwell, agreed to, among other things, and Plaintiff and Class members understood that Northwell would: (1) provide services to Plaintiff and the other Class members; (2) take

reasonable measures to protect the security and confidentiality of Plaintiff's and the other Class members' PII and PHI; and (3) protect Plaintiff's and the other Class members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

121. The protection of PII and PHI was a material term of the implied contracts between Plaintiff and the other Class members, on the one hand, and Northwell, on the other hand. Indeed, as set forth above, Northwell recognized the importance of data security and the privacy of Northwell's patients' PII and PHI. Had Plaintiff and the other Class members known that Northwell would not adequately protect their PII and PHI, they would not have received healthcare or other services from Northwell.

122. Plaintiff and the other Class members performed their obligations under the implied contract when they provided Northwell with their PII and PHI and paid for healthcare or other services from Northwell.

123. Northwell breached their obligations under their implied contracts with Plaintiff and the other Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI, including by ensuring companies they contract with implement and maintain reasonable security measures to protect PII and PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and the other

Class members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards.

124. Northwell's breach of their obligations of their implied contracts with Plaintiff and the other Class members directly resulted in the Data Breach and the injuries that Plaintiff and the other Class members have suffered from the Data Breach.

125. Plaintiff and the other Class members were damaged by Northwell's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class against all Defendants)

126. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

127. This claim is pled in the alternative to the breach of implied contract claim.

128. Plaintiff and the other Class members conferred a monetary benefit upon Defendants in the form of monies paid to Northwell for healthcare services, which Northwell used in turn to pay for PJ&A's services, and through the provision of their PII and PHI.

129. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and the other Class members. Defendants also benefitted from the receipt of Plaintiff's and the other Class members' PII and PHI, as this was used to facilitate billing services and services provided to Northwell.

130. As a result of Defendants' conduct, Plaintiff and the other Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and the other Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

131. Defendants should not be permitted to retain the money belonging to Plaintiff and the other Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and the other Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

132. Plaintiff and the other Class members have no adequate remedy at law.

133. Defendants should be compelled to provide for the benefit of Plaintiff and the other Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT, N.Y. Gen. Bus. Law § 349 ("GBL")
(On behalf of Plaintiff and the New York Subclass Against Northwell Only)

134. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

135. New York General Business Law § 349(a) states, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

136. Northwell is a "person, firm, corporation or association or agent or employee thereof" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b).

At all relevant times, Northwell was engaged in "business," "trade," or "commerce" within the meaning of the GBL. *See* N.Y. Gen. Bus. Law § 349(a).

137. Plaintiff and the other New York Subclass members are "persons" within the meaning of Gen. Bus. Law § 349(h).

138. Northwell promised to protect, but subsequently failed to adequately safeguard and maintain, Plaintiff's and the other New York Subclass members' PII and PHI. Northwell failed to notify Plaintiff and the other New York Subclass members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect their PII and PHI, including by ensuring companies it contracts with maintain adequate data protection practices.

139. Had Plaintiff and the other New York Subclass members been aware that Northwell omitted or misrepresented facts regarding the adequacy of its data security safeguards, Plaintiff and the other New York Subclass members would not have accepted services from Northwell.

140. Northwell's failure to make Plaintiff and the other New York Subclass members aware that it would not adequately safeguard their information, while maintaining that it would, is a "deceptive act or practice" under N.Y. Gen. Bus. Law § 349.

141. Plaintiff and the other New York Subclass members were damaged by Northwell's unfair and deceptive trade practices because: (i) they paid—

directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for the services that were received without adequate data security.

142. Pursuant to Gen. Bus. Law § 349(h), Plaintiff seeks damages on behalf of herself and the other New York Subclass members in the amount of the greater of actual damages or $50 for each violation of N.Y. Gen. Bus. Law § 349. Because Northwell's conduct was committed willfully and knowingly, Plaintiff and the other New York Subclass members are entitled to recover up to three times their actual damages, up to $1,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seek appropriate injunctive relief designed to prevent Defendants from permitting another data breach by adopting and implementing best data security practices to safeguard PII and PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 5, 2024

Respectfully submitted,

/s/ Nick Suciu III

Nick Suciu III (Bar No. MI P72052)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
6905 Telegraph Road, Suite 115
Bloomfield Hills, MI 48301
Tel: (313) 303-3472
nsuciu@milberg.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

James J. Pizzirusso
HAUSFELD LLP
1700 K Street, NW, Suite 650
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
(646) 357-1100
snathan@hausfeld.com

Counsel for Plaintiff and the Proposed Class